

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)

| | |
|-------|-------------|
| REC'D | 03 OCT 2000 |
| WIPO | PCT |

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

4

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **13 SEP. 2000**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

THIS PAGE BLANK (USPTO)



26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa
N° 55-1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES **16 SEPT 1 9**
N° D'ENREGISTREMENT NATIONAL **9911 94**
DÉPARTEMENT DE DÉPÔT **75** **75 INPI PARIS**
DATE DE DÉPÔT **1 6 SEP. 1999**

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

BULL S.A.
Monsieur Jean-Marc DIOU
68, route de Versailles
PC : 58F35
78434 LOUVECIENNES Cedex

n° du pouvoir permanent **PG 4972** références du correspondant **FR 3782 JMD** téléphone **01.39.66.61.81**

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire

☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

☐ demande initiale
☒ brevet d'invention

☐ certificat d'utilité n° _____ date _____

Établissement du rapport de recherche

☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

"Relais d'accès à un réseau serveur, transparent sur un réseau client"

3 DEMANDEUR (S) n° SIREN **6.4.2.0.5.8.7.3.9.**

code APE-NAF **300.C.**

Nom et prénoms (souligner le nom patronymique) ou dénomination

BULL S.A.

Forme juridique

Nationalité (s) **Française**

Adresse (s) complète (s)

Pays

BULL S.A.
68, route de Versailles
78430 LOUVECIENNES

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs

☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES

☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE

(nom et qualité du signataire)

Jean-Marc DIOU (Mandataire Bull S.A.)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Petersbourg

75800 Paris Cédex 08

Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

FR 3782 JMD

N° D'ENREGISTREMENT NATIONAL

99 M 594

TITRE DE L'INVENTION :

"Relais d'accès à un réseau serveur, transparent sur un réseau client"

LE(S) SOUSSIGNÉ(S)

BULL S.A.

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

Dujonc Jean-Yves
27 bis, avenue Pasteur
78580 Maule
France

Martin René
32, rue de Gometz
91440 Bures sur Yvette
France

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Louveciennes, le 13 septembre 1999



Jean-Marc DIOU (Mandataire Bull S.A.)

Relais d'accès à un réseau serveur, transparent sur un réseau client.

Le domaine technique auquel se rapporte l'invention est celui des réseaux informatiques. Les réseaux informatiques permettent l'exécution d'applications réparties sur des machines
5 distantes reliées à un même réseau ou reliées à des réseaux différents interconnectés au moyen de machines d'interconnexions.

Une transaction entre machines distantes est initiée par une application client qui émet un message de requête vers une application serveur en état de veille. L'application client se
10 met en état d'attente d'un message de réponse à son message de requête. A réception du message de requête, l'application serveur élabore un message de réponse qu'elle émet vers l'application client. Une couche réseau permet de véhiculer chaque message sous forme de datagramme, depuis la machine qui héberge l'application émettrice jusqu'à la machine qui héberge l'application réceptrice. Une couche transport permet de véhiculer le
15 message entre l'application émettrice et la couche réseau puis entre la couche réseau et l'application réceptrice, c'est à dire par exemple d'une application client à une application serveur. Une couche applicative concerne l'exécution de l'application dans l'environnement qui lui est propre.

Lorsque les machines ne sont pas physiquement liées au même réseau, des protocoles de
20 routage de la couche réseau acheminent les datagrammes depuis la machine émettrice vers une machine d'interconnexion et de la machine d'interconnexion vers la machine réceptrice au moyen d'adresses protocolaire inter-réseaux telles que par exemple les adresses IP. Au passage dans la machine d'interconnexion, les datagrammes restent au
25 niveau de la couche réseau. Le réseau entre la machine client et la machine d'interconnexion est appelé réseau client. Le réseau entre la machine serveur et la machine d'interconnexion est appelé réseau serveur.

Le domaine technique auquel se rapporte plus particulièrement l'invention concerne une
30 machine d'interconnexion pour héberger une application relais (proxy en anglais). Une application relais est intéressante pour effectuer des traitements sur les messages échangés entre le réseau client et le réseau serveur. Cependant, les datagrammes destinés à la machine réceptrice finale ne sont pas naturellement remontés à la couche applicative de la machine d'interconnexion.

Selon l'état de la technique antérieure connu, l'application émettrice adresse ses messages à l'application relais de la machine d'interconnexion au lieu de les adresser directement à l'application réceptrice finale et indique dans ses messages à l'application relais à quelle application finale ses messages sont destinés de sorte que l'application relais puisse les y réacheminer en fonction de traitements qu'elle leur applique. C'est ce qu'on retrouve par exemple dans un navigateur internet (browser en anglais) où il est possible de déclarer pour une application client donnée, l'adresse de la machine d'interconnexion pour la couche réseau et le numéro de port de l'application relais pour la couche transport, de sorte que le navigateur encapsule l'adresse de la machine serveur et le numéro de port de l'application destinataire finale dans un datagramme adressé à l'application relais. Cependant, cela nécessite de connaître par quelle application relais doivent passer les messages de façon à configurer la machine client en conséquence. Le manque de souplesse qui en résulte, s'il convient pour un nombre limité d'applications, n'est pas satisfaisant pour un grand nombre d'applications distinctes.

Le document RFC1928 disponible sur internet à l'adresse <http://www.pmg.lcs.mit.edu/cgi-bin/rfc/view?1928> décrit le protocole "SOCKS v5" dont le numéro de port utilisé par convention est 1080. De la même façon que pour la solution connue sous le nom "TCP protocol Tunelling in Web Proxy Servers", il est nécessaire d'établir une première connexion vers l'application relais, suivie d'une deuxième connexion de la machine relais vers la machine finale.

Pour pallier les inconvénients précédemment cités, le but de l'invention est de permettre à une application client de simplement établir une connexion vers une application serveur comme elle le ferait sans utilisation des services d'une application relais, de sorte que l'utilisation des services de l'application relais est transparente pour l'application client.

Un premier objet de l'invention est une machine d'interconnexion reliée à un réseau client au moyen d'une première interface physique et reliée à un réseau serveur au moyen d'une deuxième interface physique, caractérisée en ce qu'au moins une adresse protocolaire inter-réseaux d'une machine serveur reliée au réseau serveur, est associée à la première interface physique, et en ce qu'elle comprend une première application relais pour recevoir des datagrammes destinés à la machine serveur depuis le réseau client et pour remettre sur le réseau serveur des datagrammes à destination de la machine serveur.

Ainsi, lorsqu'un datagramme se présente sur la première interface physique avec l'adresse protocolaire inter-réseaux de la machine serveur comme adresse de destination, la machine d'interconnexion est reconnue par sa couche réseau comme étant la machine de destination du datagramme. La couche réseau de la machine d'interconnexion remonte alors le datagramme vers la couche applicative de la machine d'interconnexion par simple respect du protocole établi. Recevant ce datagramme, l'application relais peut le traiter puis le réémettre ou ne pas le réémettre vers la machine serveur. Ceci est totalement transparent pour l'application client.

Une variante de l'invention a pour objet une machine d'interconnexion reliée à un réseau client au moyen d'une première interface physique et reliée à un réseau serveur au moyen d'une deuxième interface physique, caractérisée en ce qu'au moins une adresse protocolaire inter-réseaux d'une machine serveur reliée au réseau serveur, est associée à une troisième interface physique, distincte de la première interface physique et de la deuxième interface physique et en ce qu'elle comprend une première application relais pour recevoir des datagrammes destinés à la machine serveur depuis le réseau client et pour émettre sur le réseau serveur des datagrammes à destination de la machine serveur.

Ici, le protocole de la couche réseau ne nécessite pas que l'adresse de destination soit affectée à la première interface physique qui reçoit le datagramme mais à une quelconque interface physique de la machine d'interconnexion, pour être remonté vers la couche applicative de la machine d'interconnexion.

Lorsque la machine d'interconnexion possède déjà une adresse de base sur le réseau client, utile par exemple à des protocoles de routage, ladite adresse de machine serveur est associée à la première interface physique en tant qu'adresse synonyme de l'adresse de base de la machine d'interconnexion sur le réseau client.

Un deuxième objet de l'invention est un procédé pour permettre de traiter au moyen d'une application relais exécutée dans une machine d'interconnexion entre un réseau client et un réseau serveur, des datagrammes émis sur le réseau client par une application client à destination d'une machine serveur possédant une adresse sur le réseau serveur, caractérisé en ce qu'il comprend une première étape qui associe ladite adresse sur le réseau serveur à une interface physique de la machine d'interconnexion qui n'est pas reliée au réseau serveur, de sorte que l'application relais capte les dits datagrammes.

Ceci présente l'avantage de ne pas nécessiter de configurer ou d'informer ladite application client pour que l'application relais puisse traiter les datagrammes. En effet, l'application client continue à émettre ses datagrammes en utilisant l'adresse de la machine serveur. Lorsque le datagramme arrive sur la première interface physique de la machine d'interconnexion, le protocole réseau fait que le datagramme remonte naturellement vers la couche applicative de la machine d'interconnexion, permettant ainsi à l'application relais de le capter.

Dans le cas où il est nécessaire de router par la machine d'interconnexion, les datagrammes transmis du réseau client au réseau serveur, le procédé est caractérisé en ce que la première étape est précédée d'une deuxième étape pour router les datagrammes transmis sur le réseau client à destination de la machine serveur, vers la machine d'interconnexion. C'est par exemple le cas lorsque la machine d'interconnexion entre le réseau client et le réseau serveur n'est pas unique.

D'autres avantages et détails de mise en œuvre de l'invention ressortent de la description qui suit en référence aux figures où:

- la figure 1 représente un exemple de machine d'interconnexion à deux interfaces physiques;
- la figure 2 représente un exemple de datagramme;
- la figure 3 représente un exemple de machine d'interconnexion à trois interfaces physiques.

Sur la figure 1 sont représentées des machines serveur 1, 2 et des machines client 11, 12.

Les machines 1, 2, 11, sont reliées à un réseau serveur 3 au moyen d'interfaces physiques respectives 7, 8, 17. Une machine client 12 est reliée à un réseau client 13 au moyen d'une interface physique 18. Les réseaux 3 et 13 sont physiquement distincts. Une machine d'interconnexion 4 est reliée au réseau serveur 3 au moyen d'une interface physique 14 et au réseau 13 au moyen d'une interface physique 19.

Des applications 5, 6, 15, 16, exécutées dans les machines 1, 2, 11, 12, communiquent entre elles au moyen d'une couche transport CT selon un protocole en mode non connecté tel que UDP ou en mode connecté tel que TCP. La couche transport CT supervise une couche réseau CR selon un protocole tel que IP.

Dans la couche réseau CR, la machine 1 est reconnue au moyen d'une adresse @S1, la machine 2 est reconnue au moyen d'une adresse @S2, la machine 11 est reconnue au moyen d'une adresse @C1. De façon connue, chacune des adresses @S1, @S2 et @C1 possède un champ réseau avec une valeur commune qui identifie le réseau 3 et un champ machine avec une valeur distincte qui identifie chaque machine liée au réseau 3. La machine 12 est reconnue au moyen d'une adresse @C2 avec une valeur de champ réseau qui identifie le réseau 13 et une valeur de champ machine qui identifie la machine 12 sur le réseau 13. La machine 4 est reconnue au moyen d'une adresse @P1 avec une valeur de champ réseau qui identifie le réseau 13 et une valeur de champ machine qui identifie la machine 4 sur le réseau 13 et au moyen d'une adresse @P2 avec une valeur de champ réseau qui identifie le réseau 3 et une valeur de champ machine qui identifie la machine 4 sur le réseau 3.

Les machines communiquent entre elles au moyen de messages qui circulent sur les réseaux sous forme de datagrammes. La figure 2 présente un exemple de datagramme. Ce datagramme, constitué d'une trame de bits successifs, est structuré essentiellement en trois champs successifs. Un premier champ repéré DR est destiné au protocole de la couche réseau. Un deuxième champ repéré DT est destiné au protocole de la couche transport qui supervise la couche réseau. Un troisième champ repéré DA est destiné à une couche applicative qui supervise la couche transport. Dans le cas d'une requête sur la toile (web en anglais) par exemple, le champ DR contient les adresses IP source et destination, le champ DT contient les numéros de port TCP source et destination, le champ DA contient des données HTTP.

Par exemple, si une application client 15 exécutée dans la machine client 11, effectue une requête d'accès à un fichier traité par une application serveur 5 située dans la machine serveur 1, l'application 5 transmet sa requête à la couche CT de la machine 11 qui écrit la requête dans le champ DA et qui écrit dans le champ DT, un numéro de port de service pour l'application 15 et un numéro de port de service pour l'application 5. La couche CT de la machine 11 transmet les champs DT et DA à la couche CR de la machine 11 qui écrit dans le champ DR, l'adresse @C1 de la machine 11 et l'adresse @S1 de la machine 1. La couche CR transmet ensuite le datagramme ainsi constitué à l'interface 17 qui arrive sur l'interface 7 de la machine 1. La couche CR de la machine 1 reconnaît par l'adresse @S1 que le datagramme est destiné aux couches supérieures de la machine 1 et retransmet les champs DT et DA à la couche CT de la machine 1. Au moyen du numéro de port de service

pour l'application 5, la couche CT retransmet le champ DA à l'application 5 qui traite la requête.

Si une application 16 exécutée dans la machine client 12, effectue une requête d'accès à un fichier traité par l'application 5 située dans la machine serveur 1, l'application 16 transmet sa requête à la couche CT de la machine 12 qui l'écrit dans le champ DA et qui écrit dans le champ DT, un numéro de port de service pour l'application 16 et un numéro de port de service pour l'application 5. La couche CT de la machine 12 transmet les champs DT et DA à la couche CR de la machine 12 qui écrit dans le champ DR, l'adresse @C2 de la machine 12 et l'adresse @S1 de la machine 1. La couche CR transmet ensuite le datagramme ainsi constitué à l'interface 18 qui arrive sur l'interface 19 de la machine 4, déclarée comme routeur entre les réseaux 13 et 3.

En absence de dispositif selon l'invention, l'adresse @S1 n'étant pas une adresse de destination de la machine 4, la couche CR de la machine 4 reconnaît que le datagramme n'est pas destiné aux couches supérieures de la machine 4. La couche CR de la machine 4 recherche alors dans des tables de routage une ligne contenant une valeur identique au champ réseau de l'adresse @S1. La ligne ainsi trouvée indique alors l'interface 14 comme étant celle d'accès au réseau 3. La couche CR de la machine 4 retransmet alors le datagramme sur le réseau 3 par l'interface 14 de sorte que le datagramme arrive sur l'interface 7 de la machine 1. La couche CR de la machine 1 reconnaît par l'adresse @S1 que le datagramme est destiné aux couches supérieures de la machine 1 et retransmet les champs DT et DA à la couche CT de la machine 1. Au moyen du numéro de port de service pour l'application 5, la couche CT retransmet le champ DA à l'application 5 qui traite la requête.

Avec le dispositif selon l'invention, la machine 4 comprend une application 22 qui joue le rôle de relais (proxy server en anglais) pour des requêtes en provenance du réseau 13. L'application 22 présente plusieurs avantages, par exemple elle peut effectuer un contrôle d'accès aux machines 1, 2, 11 reliées au réseau serveur 3, elle peut sauvegarder des réponses à des requêtes précédentes dans une antémémoire (cache en anglais) pour restituer ces réponses à de nouvelles requêtes sans nécessiter d'acheminer ces nouvelles requêtes jusqu'à la machine serveur 1, 2.

Plusieurs adresses de la couche CR sont associées à l'interface physique 19, d'un part l'adresse habituelle @P1 et d'autre part l'adresse @S1 de la machine serveur 1 reliée au

réseau 3. Il est possible aussi d'associer l'adresse @S2 d la machine serveur 2 à l'interface physique 19. Comme il ressort de la suite de la description, à la différence de l'état de la technique où c'est le réseau client qui détermine l'utilisation des services de l'application relais 22, c'est ici le réseau serveur qui détermine cette utilisation par exemple l'accès au serveur 1 en associant l'adresse @S1 à l'interface physique 19.

L'application 22 comprend un port d'entrée 9 de numéro identique au port d'entrée de l'application 5 et un port de sortie 10 auquel elle a la possibilité d'attribuer un numéro pour gérer des messages de requête éventuels à destination de l'application 5.

Grâce à ce dispositif particulier, la machine 12 n'a pas besoin de savoir qu'elle établit une connexion intermédiaire avec la machine 4. Si une application 16 exécutée dans la machine client 12, effectue une requête destinée à l'application 5 située dans la machine serveur 1, l'adresse @S1 est maintenant reconnue sur le réseau 13 comme étant celle de la machine 4.

Pour effectuer une requête destinée à l'application 5, l'application 16 envoie un datagramme Q sur le réseau 13 qui contient dans le champ CR, les adresses @S1 et @C2, dans le champ transport, les numéros de port des applications 5 et 16, dans le champ CA, les informations finales destinées à l'application 5.

Lorsque le datagramme Q est reçu sur l'interface physique 19 de la machine 4, la couche réseau CR de la machine 4 reconnaît l'adresse de destination @S1 dans le champ DR comme étant une adresse qui lui est propre et remonte donc le datagramme vers la couche transport CT de la machine 4. La couche transport CT reconnaît le numéro de destination dans le champ DT comme étant le numéro du port 9 de l'application 22 à laquelle elle transmet alors le contenu du datagramme Q.

L'application 22 traite alors le contenu du champ DA du datagramme Q. Le traitement du datagramme Q par l'application 22 consiste par exemple à vérifier des droits d'accès, à vérifier si la machine 4 contient déjà une réponse à la requête dans son antémémoire pour décider de communiquer ou de ne pas communiquer le datagramme Q à l'application serveur 5.

Lorsque pour traiter le message de requête en provenance de l'application client 16, l'application 22 a besoin d'émettre un message de requête vers l'application 5, l'application

22 communique les données suivantes à la couche transport CT de la machine 4, le contenu de la requête à mettre dans le champ DA, le numéro de port d'entrée de l'application 5, un numéro de port de sortie de l'application 22 pour gérer la réponse à la requête, l'adresse protocolaire inter-réseau @S1 de la machine 1. Ces données sont transmises à la couche réseau CR de la machine 4. A réception de ces données, la couche réseau CR de la machine 4 recherche dans ses tables de routages sur quel réseau émettre un datagramme, en fonction du champ réseau de l'adresse @S1. Dans l'exemple ici décrit, le champ réseau de l'adresse @S1 correspondant au réseau 3 auquel est reliée la machine 1, la couche CR émet vers l'interface physique 14, un datagramme contenant dans le champ DR, l'adresse de destination @S1 et l'adresse source @P2 associée à l'interface physique 14. Sur le réseau serveur 3, le datagramme parvient de façon classique jusqu'à la machine 1 et jusqu'à l'application serveur 5 dans la machine 1.

La réponse reçue de l'application 5 sur l'interface 14 est remontée à l'application 22 par la couche réseau car l'adresse @P2 est une adresse de la machine 4, et par la couche transport CT car le numéro de port pour la réponse est celui attribué sur le port 10 par l'application 22. Au moyen d'un mécanisme interne de gestion de requêtes et de réponses, l'application 22 associe la réponse au numéro de port de sortie reçu de l'application 16. Pour réémettre la réponse vers l'application 16, l'application 22 communique les données suivantes à la couche transport CT de la machine 4, le contenu de la réponse à mettre dans le champ DA, le numéro de port de sortie de l'application 16, le numéro de port d'entrée de l'application 22 qui est identique au numéro de port d'entrée de l'application 5 pour gérer la réponse à la requête, l'adresse protocolaire inter-réseau de destination @C2 de la machine 12 et l'adresse protocolaire inter-réseau source @S1 de la machine 1. Ces données sont transmises à la couche réseau CR de la machine 4 par la couche transport. A réception de ces données, la couche réseau CR de la machine 4 recherche dans ses tables de routages sur quel réseau émettre un datagramme, en fonction du champ réseau de l'adresse @C2. Dans l'exemple ici décrit, le champ réseau de l'adresse @C2 correspondant au réseau 13 auquel est reliée la machine 12, la couche CR émet vers l'interface physique 19, un datagramme contenant dans le champ DR, l'adresse de destination @P2 et l'adresse source @S1 associée à l'interface physique 19. Sur le réseau client 13, le datagramme parvient de façon classique jusqu'à la machine 12 et jusqu'à l'application client 16 dans la machine 1.

Ainsi, l'application 16 dans la machine 12 voit revenir une réponse en provenance de l'application 5 dans la machine 1 sans voir son transit par l'application 22 qui s'est fait de façon transparente pour l'application client 16.

- 5 En référence à la figure 3, l'adresse @S1 est associée à une interface physique 20 différente tant de l'interface 14 comme précédemment que de l'interface 19 comme ici particulièrement.

10 Lorsqu'un datagramme est émis sur le réseau 13 avec l'adresse @S1, le protocole de routage de la couche réseau CR de la machine 4 le capte sur l'interface 19 à laquelle est associée l'adresse @P1. Comme l'adresse @S1 associée à l'interface physique 20, est une adresse de la machine 4, le datagramme est remonté à la couche applicative CA de la machine 4.

- 15 Une application relais 21 traite le message de requête issu du datagramme reçu, de façon identique à l'application relais 22 précédente. Pour émettre le message de réponse vers l'application 12, l'application relais 22 dispose d'un pilote particulier vers un réseau virtuel auquel est reliée l'interface physique 20.

- 20 Le cas où l'adresse IP @S1 est associée à l'interface 19 est particulièrement avantageuse pour la facilité de mise en œuvre de l'invention. Dans l'exemple simple qui suit, l'application 16 exécute une fonction Telnet en tant qu'application cliente, l'application 22 exécute une fonction telnetd en tant qu'application serveur de l'application 16 et une fonction Telnet en tant que client de l'application 5. L'application 5 exécute une fonction telnetd en tant que
- 25 serveur de l'application 22. Telnet et telnetd sont des fonctions connues, utilisant TCP/IP pour connecter un terminal de machine client où s'exécute la fonction Telnet, à une machine serveur où s'exécute la fonction telnetd.

- 30 De façon à suivre sur quelle machine sont exécutées les commandes, chacune tourne sur un système d'exploitation différent. La machine client 12 tourne sur un système AIX (marque déposée) de version 4.1 et possède comme adresse IP: @C1 = 129.182.51.58. La machine relais 4 tourne sur un système AIX de version 4.2 et possède comme adresses IP: @P1 = 129.182.51.21 et @P2 = 192.90.249.22. La machine serveur 12 tourne sur un système DNS-E (propriétaire) et possède comme adresse IP: @S1 = 192.90.249.124. Le
- 35 réseau 13 est accessible de façon connue par une adresse IP: @R1 = 129.182.50 avec un masque @M1 = 255.255.254.0.

Sur la machine client 12, la commande:

```
route add -host 192.90.249.124 129.182.51.21
```

définit que pour atteindre la machine serveur 1 d'adresse @S1, les datagrammes émis
5 passent par la machine relais d'adresse @P1.

Sur la machine serveur 1, la commande:

```
route add -net 129.182.50 192.90.249.22 -netmask 255.255.254.0
```

définit que pour atteindre toute machine du réseau 13 d'adresse @R1, les datagrammes
10 émis passent par la machine relais d'adresse @P2.

Sur la machine client 12, la commande:

```
Telnet 192.90.249.124
```

active l'application Telnet pour atteindre la machine serveur 1 d'adresse @S1. A ce stade,
15 la seule machine reconnue par l'adresse IP @S1 est la machine serveur 1. La couche IP de
la machine 4 route les datagrammes émis par la couche IP de la machine 12, vers la
couche IP de la machine serveur 1. La couche IP de la machine 1 reconnaissant l'adresse
@S1, remonte le champ applicatif des datagrammes vers l'application telnetd de la
machine 1. L'application telnetd de la machine 1 émet en retour vers la machine 12, le
20 message:

```
Trying...
```

```
Connected to 192.90.249.124.
```

```
Escape character is '^]'.
```

```
$$ 0000 *DNS-E V3U1.000 P1.001 P2.019 P3.010*IMA:BX77SIM 1998/10/21
```

```
17:23*
```

L'affichage de ce message sur le terminal de la machine 12, montre que celui-ci est dans
l'environnement du système DNS, c'est à dire qu'on atteint directement la machine 1. La
machine relais 4 n'a été traversée que pour réaliser le routage IP.

30 Sur la machine client 12, la commande:

```
Telnet 129.182.51.21
```

active l'application Telnet pour atteindre la machine relais 4 d'adresse @P1. La couche IP
de la machine 4 reconnaissant l'adresse @P1, remonte le champ applicatif des
datagrammes vers l'application telnetd de la machine 4. L'application telnetd de la machine
35 4 émet en retour vers la machine 12, le message:

```
Trying...
```

Connected to 129.182.51.21.

Escape character is '^['.

Telnet (treize)

AIX Version 4

© Copyrights by IBM and by others 1982, 1996.

Login:

L'affichage de ce message sur le terminal de la machine 12, montre que celui-ci est dans l'environnement du système AIX, c'est à dire qu'on atteint la machine 4. Ceci permet de générer des commandes depuis le terminal de la machine 12 qui sont exécutées dans la machine 4.

Sur la machine 4, l'interface 19 étant nommée en1, la commande:

ifconfig en1 192.90.249.124 alias

définit l'adresse @S1 comme une adresse supplémentaire associée à l'interface 19. La machine 4 ne risque pas d'être confondue avec la machine 1 sur le réseau 13 par la couche IP, car celui-ci est physiquement distinct du réseau 3. De même, la commande:

ifconfig en1 192.90.249.125 alias

définirait l'adresse @S2 comme une adresse supplémentaire associée à l'interface 19.

Revenant sur la machine 12, la commande:

Telnet 192.90.249.124

active alors l'application Telnet avec un effet différent de celui décrit précédemment. Le message affiché sur le terminal de la machine 12 est:

Trying...

Connected to 129.182.51.21.

Escape character is '^['.

Telnet (treize)

AIX Version 4

© Copyrights by IBM and by others 1982, 1996.

Login:

L'affichage de ce message sur le terminal de la machine 12, montre que celui-ci est dans l'environnement du système AIX de la machine 4. Bien qu'ayant demandé une connexion à l'application telnetd de la machine serveur 1 au moyen de l'adresse @S1, la commande a effectué une connexion à l'application telnetd de la machine 4. Ceci s'explique par le fait que la couche IP de la machine 4 reconnaît l'adresse @S1 comme une adresse de destination propre à la machine 4, sans tenir compte du routage vers le réseau 3. Ainsi, la

couche IP de la machine 4 remonte le champ applicatif des datagrammes reçus sur l'interface 19, vers l'application telnetd de la machine 4.

A présent sur la machine 4, la commande:

```

5                               Telnet 192.90.249.124
active l'application Telnet pour atteindre la machine serveur 1 d'adresse @S1. A ce stade,
la seule machine reconnue par l'adresse IP @S1 à partir de l'interface 14, est la machine
serveur 1. La couche IP de la machine 1 reconnaissant l'adresse @S1, remonte le champ
applicatif des datagrammes vers l'application telnetd de la machine 1. L'application telnetd
10 de la machine 1 émet en retour vers l'application Telnet de la machine 4, le message:
    Trying...
    Connected to 192.90.249.124.
    Escape character is '^J'.
    $$ 0000 *DNS-E V3U1.000 P1.001 P2.019 P3.010*IMA:BX77SIM 1998/10/21
15    17:23*
```

Ce message est retransmis par l'application telnetd de la machine 4 vers l'application Telnet de la machine 12. L'affichage de ce message sur le terminal de la machine 12, montre qu celui-ci est dans l'environnement du système DNS, c'est à dire qu'on atteint la machine 1. Cependant, le champ applicatif des datagrammes est remonté à la couche applicative de la machine relais 4, de façon transparente pour la machine 12.

Le procédé qui vient d'être expliqué au moyen d'une manipulation manuelle, peut être réalisé au moyen d'un programme exécuté par la couche applicative de la machine 4.

25 Les datagrammes à destination de la machine 1, passant par la couche IP de la machine 4, sont remontés dans la couche applicative de la machine 4 car l'adresse @S1 est associée à une interface physique de la machine 4. Pour éviter des conflits sur le réseau 3 avec la machine 1, il est préférable de ne pas associer l'adresse @S1 à l'interface 14. En référence à la figure 3, il est possible d'associer l'adresse @S1 à une autre interface physique que

30 l'interface 19, par exemple à une interface physique 20.

Un exemple de traitement particulier par l'application 22 décrit ici, présente un avantage particulier. Dans le cas où des clés de cryptage sont associées à l'adresse @S1 pour chiffrer les requêtes en provenance et les réponses à destination de la machine 12, le

35 décryptage des requêtes et le cryptage des réponses peut être assuré par la machine 4. Les données peuvent circuler décryptées sur le réseau serveur 3 sans risque. Ainsi, les

ressources de cryptage et décryptage peuvent être centralisées dans la machine 4 en laissant un maximum de ressources disponibles à la machine 1 pour ses fonctions de serveur. L'application 22 se charge aussi de recrypter les réponses avant de les émettre sur le réseau 13.

REVENDEICATIONS:

1. Machine d'interconnexion (4) reliée à un réseau client (13) au moyen d'une première interface physique (19) et reliée à un réseau serveur (3) au moyen d'une deuxième interface physique (14), caractérisée en ce qu'au moins une adresse protocolaire inter-réseaux (@S1, @S2) d'une machine serveur (1, 2) reliée au réseau serveur (3), est associée à la première interface physique (19), et en ce qu'elle comprend une première application relais (22) pour recevoir des datagrammes destinés à la machine serveur (1, 2) depuis le réseau (13) et pour émettre sur le réseau (3) des datagrammes à destination de la machine serveur (1,2).

2. Machine d'interconnexion (4) reliée à un réseau client (13) au moyen d'une première interface physique (19) et reliée à un réseau serveur (3) au moyen d'une deuxième interface physique (14), caractérisée en ce qu'au moins une adresse protocolaire inter-réseaux (@S1, @S2) d'une machine serveur (1, 2) reliée au réseau serveur (3), est associée à une troisième interface physique (20), distincte de la première interface physique (19) et de la deuxième interface physique (14) et en ce qu'elle comprend une première application relais (22) pour recevoir des datagrammes destinés à la machine serveur (1, 2) depuis le réseau (13) et pour émettre sur le réseau (3) des datagrammes à destination de la machine serveur (1,2).

3. Machine d'interconnexion (4) selon la revendication 1, caractérisée en ce que ladite adresse (@S1, @S2) est associée à la première interface physique (19) en tant qu'adresse synonyme d'une adresse de base (@P1) de la machine (4) sur le réseau (13).

4. Procédé pour permettre de traiter au moyen d'une application relais (22) exécutée dans une machine d'interconnexion (4) entre un réseau client (13) et un réseau serveur (3), des datagrammes émis sur le réseau client (13) par une application client (16) à destination d'une machine serveur (1) d'adresse (@S1) sur le réseau serveur (3), caractérisé en ce qu'il comprend une première étape qui associe ladite adresse (@S1) à une interface physique (19, 20) de la machine d'interconnexion (4) qui n'est pas reliée au réseau serveur (3), de sorte que l'application relais (22) capte les dits datagrammes sans nécessiter de configurer ou d'informer ladite application client (16) à cette fin.

5. Procédé selon la revendication 4, caractérisé en ce que la première étape est précédé d'une deuxième étape pour router les datagrammes transmis sur le réseau client (13) à destination de la machine serveur (1), vers la machine d'interconnexion (4).

5 6. Machine d'interconnexion (4) selon la revendication 1 ou 2, caractérisée en ce que l'application (22) dispose de clés de cryptages de façon à transmettre déchiffrés sur le réseau 3, des messages chiffrés en provenance du réseau 13.

10 7. Machine d'interconnexion (4) selon la revendication 1 ou 2, caractérisée en ce que l'application (22) dispose de clés de cryptages de façon à transmettre chiffrés sur le réseau 13, des messages non chiffrés en provenance du réseau 3.

Fig.1

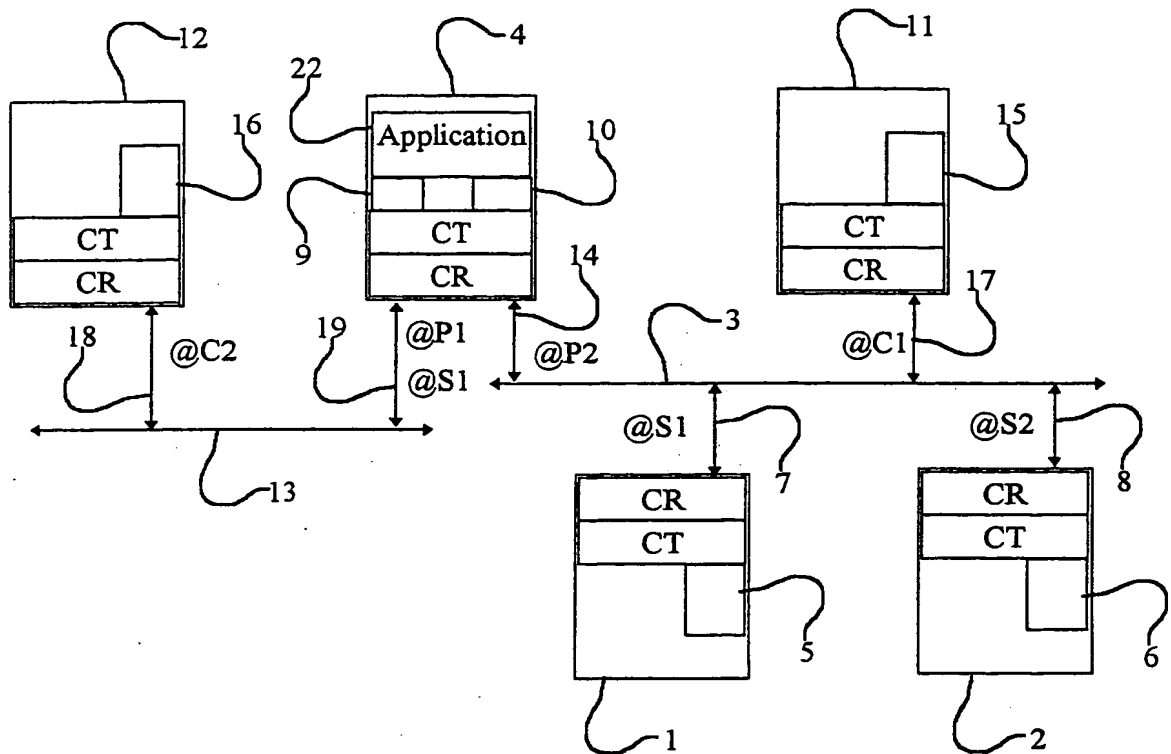


Fig.2

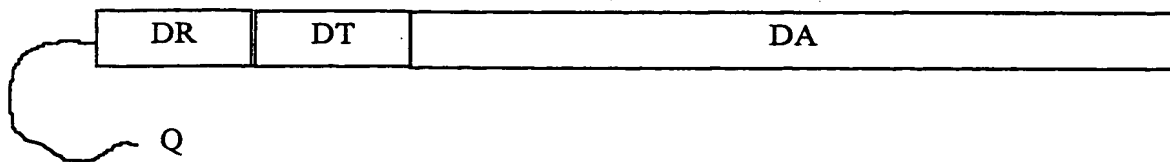
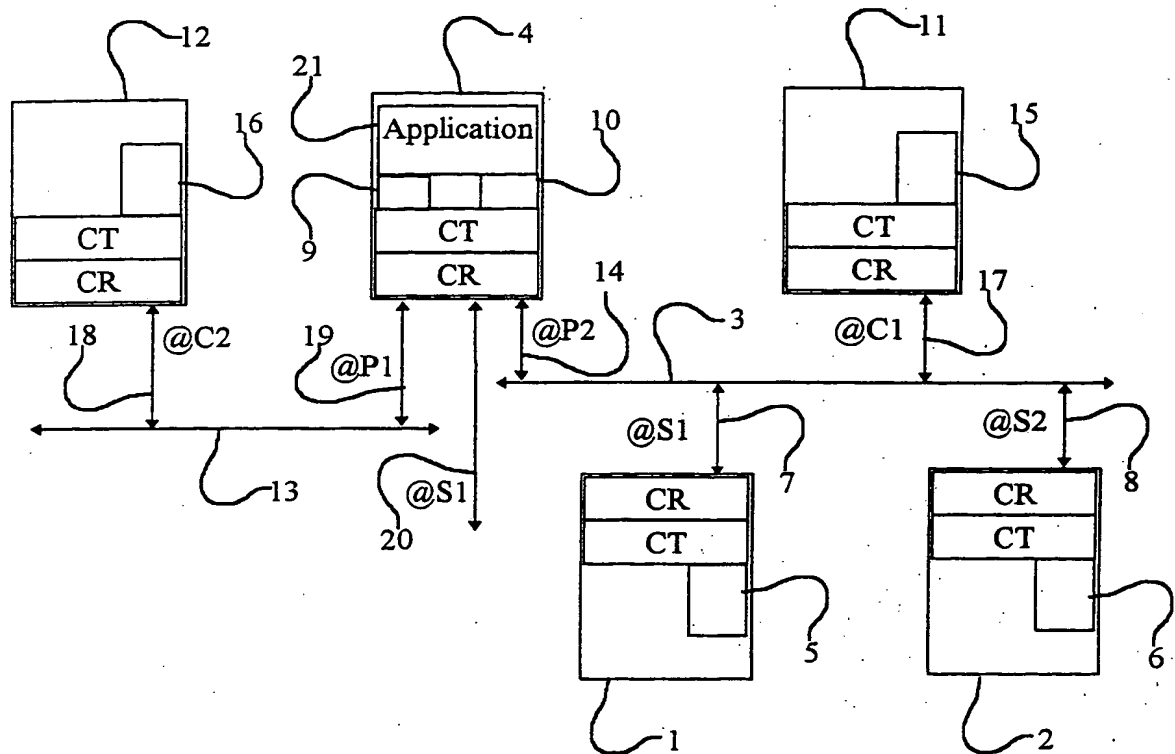


Fig.3



THIS PAGE BLANK (USPTO)
